



### Lisa Sotto

Partner

Hunton Andrews Kurth



United States of America

**In terms of career highlights so far**, my team at Hunton has worked on the most notable cybersecurity incidents globally, whether measured in terms of real-world impact or the number of people affected. Specifically, we helped Colonial Pipeline navigate the cyberattack that resulted in the shutdown of its pipeline for six days. My team also handled all aspects of the cybersecurity attacks against Yahoo!, which were carried out by state-sponsored actors and compromised more than three billion user accounts. In an interview with the *Penn Law Journal*, Dan Tepstein, senior managing associate general counsel at Verizon who was at Yahoo! when the breaches occurred, said: “I don’t know of any other lawyer or firm who has had more significant experience in [data breaches], or dealt with [these] types of high-profile breaches.”

I admit to getting a kick out of being known as the “queen of breach.”

Beyond nicknames or specific incidents, I’m most proud of the privacy and cybersecurity team I have helped to build from the ground up. Hunton was among the first US law firms to enter the privacy arena, creating the practice in 2000. Starting with a very small team, we have grown to over 45 lawyers and privacy professionals globally. Complementing the legal practice is our privacy think tank, the Centre for Information Policy Leadership (CIPL), which operates at the leading edge of privacy policy and data innovation globally. CIPL often works alongside our privacy lawyers on data-driven projects for Hunton clients and CIPL members.

**In terms of challenges**, with cybersecurity incidents and data breaches, a rapid response is essential. Once a breach is detected, the first 24 to 36 hours are critical to its resolution. Often when we get the call from a client, very little is known about the nature and scope of the incident. While we are ensuring that our client is meeting its legal obligations, we are simultaneously working hard to address the vulnerability that the threat actor exploited and, most importantly, get the company's systems up and running. These are all significant challenges that must be met quickly to avoid lasting harm.

**Preparation is key.** Organisations should practice managing a cyberattack through tabletop exercises, and ensure that they have a state-of-the-art incident response plan to serve as a roadmap when the real thing hits. In addition, members of the incident response team should be well aware of their roles and responsibilities in the event of a cyberattack. Preparing to handle an incident in advance will mitigate harm to the organisation in the event of an actual breach.

**This is an extraordinary time for professionals in the fields of privacy and cybersecurity.** Privacy laws in the US are evolving quickly. California, Virginia and Colorado recently enacted comprehensive privacy laws, and other states are likely to follow. This will inevitably lead to a comprehensive federal data protection law, which I am hoping will come sooner rather than later.

Of course, it's not just the law that's changing – dynamic technological forces like artificial intelligence, blockchain technology, and cryptocurrency will keep us on our toes as we grapple with their privacy and security implications. Additionally, ransomware attacks will undoubtedly continue unabated in 2022. We can anticipate seeing even more sophisticated and devastating cyberattacks on businesses that are not prepared.

**Privacy has always been an area replete with women leaders.** That's not the case for cybersecurity, where I'm still often the only woman in the room. While we have seen a small increase in women cybersecurity leaders over the last decade, female representation is still low.

**A piece of advice I would give aspiring data lawyers and professionals is to** keep pursuing this amazing career. It offers a wealth of opportunity as technology and information practices continue to evolve. And remember that relationships are incredibly important. Keep building those that you have, and cultivate new ones as you progress in your career.